PTO/SB/44 (09-07)
Approved for use through 08/31/2013. OMB 0651-0033
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

(Also Form PTO-1050)

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

Page 1 of 2

PATENT NO. : 7,657,748 B2

APPLICATION NO.: 10/521,741

ISSUE DATE : February 2, 2010

INVENTOR(S) : Craig B. Gentry

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 8, Line 34: delete "(PKB, SKB)"; insert --(PK_B, SK_B)--.

Column 8, Line 44: delete the word "params"; insert --*params*--.

Column 8, Line 45: delete the words "masks S"; insert --masks *s*--.

Column 8, Line 46: delete the word "ID"; insert --*ID*--.

Column 8, Line 50 & 51: delete the words "s, params and ID"; insert --*s, params* and *ID*--.

Column 8, Line 52: delete the word "ID"; insert --*ID*--.

Column 8, Line 54: delete the words "params, ID and M"; insert --*params, ID* and *M*--

Column 8, Line 55: delete the words "C to recover M"; insert --*C* to recover *M*--

Column 10, Line 61 & 62: delete "ê(P, P)^{abc} if P, aP, bP, and cP are known, but a, b, and c are not";
insert --$\hat{e}(P, P)^{abc}$ if P, aP, bP, and cP are known, but a, b, and c are not--.

Column 10, Line 64 & 65: delete "ê(P, P)^{abc} = ê(abP, cP)";
insert -- $\hat{e}(P, P)^{abc} = \hat{e}(abP, cP)$--

Column 10, Line 66 & 67: delete "g= ê(P, P), then g^{abc}=g^{ab})^{c} where g^{ab}= ê(aP, bP) and g^{c}= ê(P, cP)"
insert --$g= \hat{e}(P, P)$, then $g^{abc}=(g^{ab})^c$ where $g^{ab}= \hat{e}(aP, bP)$ and $g^c= \hat{e}(P,cP)$--

Column 11, Line 48: delete "C = [rP, M ⊕ H$_2$(g^r)], where g=ê(Q, P$_B$)∈ G$_2$";
insert --C = [rP, M⊕H$_2$(g^r)], where g = ê(Q, P$_B$)ê(s$_B$P, P'_B)∈ G$_2$--

Column 12, Line 59: delete the word "params"; insert --*params*--.

Column 13, Line 39: delete the word "params"; insert --*params*--.

MAILING ADDRESS OF SENDER (Please do not use customer number below):

Michael Shenker
Haynes and Boone, LLP
IP Section
2323 Victory Avenue, Suite 700
Dallas, Texas 75219

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/44 (09-07)
Approved for use through 08/31/2013. OMB 0651-0033
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.
(Also Form PTO-1050)

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

Page 2 of 2

PATENT NO. : 7,657,748 B2

APPLICATION NO.: 10/521,741

ISSUE DATE : February 2, 2010

INVENTOR(S) : Craig B. Gentry

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 13, Line 43: delete the word "Musing"; insert --*M* using--

Column 15, Line 7: delete the word "sendery"; insert --sender *y*--

Column 15, Line 11: delete the word "sendery"; insert --sender *y*--

Column 15, Line 60: delete "m-1+1"; insert --m-l +1--

Column 15, Line 66: delete "1-1"; insert --l -1--

Column 16, Line 10: delete "n-1+1"; insert --n-l +1--

Column 16, Line 17: delete "1-1"; insert --l -1--

Column 16, Line 25: delete "n-1"; insert --n-l--

Column 19, Line 37: delete "sendery"; insert --sender *y*--

Column 20, Line 19: delete "$\mathrm{U_1=rP}_{zi}$ for $\mathrm{k+1 \leqq I \leqq n+1}$";
insert -- $U_i=rP_{zi}$ for $l+1 \leq i \leq n+1$--

Column 24, Line 40: delete the word "params"; insert --*params*--.

Claim 80 line 8 (Column 38, Line 11): delete "key!recipient"; insert --key/recipient--.

Claim 80 line 21 (Column 38, Line 24): delete "key!private"; insert --key/private--.

MAILING ADDRESS OF SENDER (Please do not use customer number below):

Michael Shenker
Haynes and Boone, LLP
IP Section
2323 Victory Avenue, Suite 700
Dallas, Texas 75219

This collection of information is required by 37 CFR 1.322, 1.323, and 1.324. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1.0 hour to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Attention Certificate of Corrections Branch, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.